

09/46 15 S99P0494 WO00

PCT/JP99/02404

日 本 国 特 許 庁

PATENT OFFICE

JAPANESE GOVERNMENT

REC'D 21 MAY 1999 10.05.99

WIPO PCT

EKU

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1998年 5月11日

出 願 番 号

Application Number:

平成10年特許願第127227号

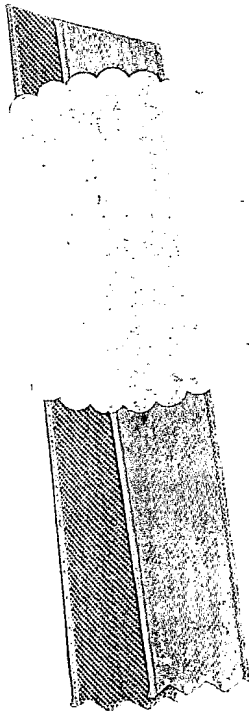
出 願 人

Applicant(s):

ソニー株式会社

**PRIORITY  
DOCUMENT**

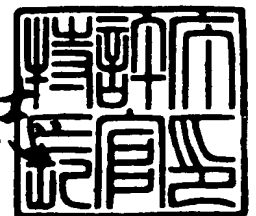
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)



1999年 3月26日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3019382

【書類名】	特許願
【整理番号】	9800055702
【提出日】	平成10年 5月11日
【あて先】	特許庁長官 荒井 寿光 殿
【国際特許分類】	H04L 12/00
【発明の名称】	情報配信システム
【請求項の数】	7
【発明者】	
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
	内
【氏名】	勝又 泰
【発明者】	
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
	内
【氏名】	大林 正之
【発明者】	
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
	内
【氏名】	中津山 孝
【発明者】	
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
	内
【氏名】	韓 敏哉
【特許出願人】	
【識別番号】	000002185
【氏名又は名称】	ソニー株式会社
【代表者】	出井 伸之
【代理人】	
【識別番号】	100082762

【弁理士】

【氏名又は名称】 杉浦 正知

【電話番号】 03-3980-0339

【手数料の表示】

【予納台帳番号】 043812

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社

---

-----【書類名】-----職権訂正データ-----  
【訂正書類】特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】000002185  
【住所又は居所】東京都品川区北品川6丁目7番35号  
【氏名又は名称】ソニー株式会社

【代理人】

申請人  
【識別番号】100082762  
【住所又は居所】東京都豊島区東池袋1-48-10 25山京ビル  
420号 杉浦特許事務所  
【氏名又は名称】杉浦 正知

【書類名】 明細書

【発明の名称】 情報配信システム

【特許請求の範囲】

【請求項 1】 複数のデータが蓄積されるとともに上記複数のデータの各々に相対する固有情報が蓄積される第 1 の記憶手段と、

上記複数のデータのうち所定のデータに相対する上記固有情報を用いて上記所定のデータを暗号化する暗号化手段と、

暗号化された上記所定のデータ及び上記所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

上記送信手段により送信された上記暗号化された所定のデータ及び上記所定のデータに相対する固有情報を受信する受信手段と、

少なくとも上記受信された上記固有情報を蓄積する第 2 の記憶手段と、

上記暗号化された所定のデータに相対する固有情報により復号化する復号化手段と、

上記受信手段により受信された上記固有情報を上記第 2 の記憶手段に予め記憶された他の上記固有情報と比較する比較手段と、

上記比較手段の判別に応じて課金処理を行う課金処理手段とを有する端末装置と

を備える情報配信システム。

【請求項 2】 上記比較手段により、上記受信手段により受信された上記固有情報が上記第 2 の記憶媒体により予め記憶されていると判断されるとき、上記課金処理手段による課金処理を禁止するようにした請求項 1 に記載の情報配信システム。

【請求項 3】 上記受信手段による受信された上記固有情報に応じて上記課金処理の金額を決定するようにした請求項 1 に記載の情報配信システム。

【請求項 4】 ユーザが有するユーザ固有情報が上記端末装置から上記情報センタに送信され、上記情報センタにおいて上記暗号化された所定のデータ及び上記所定のデータに相対する固有情報を各々上記ユーザ固有情報に暗号化されて

【書類名】 要約書

【要約】

【課題】 コンテンツの配信を行なうようなシステムで、コンテンツの保護が十分図れ、正当な課金が行なえるようにする。

【解決手段】 コンテンツサーバ 101 には、Cキーにより暗号化されたコンテンツと、Cキーとが蓄積されるコンテンツデータベース 111 を設ける。このCキーにより暗号化されたコンテンツと、Cキーを、Mキーで暗号化して、ユーザマシン 102 に送る。ユーザマシン 102 では、Cキーにより暗号化されたコンテンツと、Cキーをストレージデバイス 120 に保存する。再生時にストレージデバイス 120 からのCキーにより暗号化されたコンテンツと、Cキーを、暗号化／復号化処理チップ 121 に送り、復号すると共に、Cキーに応じて、課金を行う。また、Cキーに、時間と共に動的に変化するDAコードを付加する。このようなDAコードを付加することで、Cキーを退避させておいて、コンテンツを不正利用するようなことが防止できると共に、DAコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

【選択図】 図 3

上記端末装置に送信され、端末装置においてユーザ固有情報により復号化されるようにした請求項 1 に記載の情報配信システム。

【請求項 5】 複数のデータが蓄積されるとともに上記複数のデータの各々に相対する固有情報が蓄積される第 1 の記憶手段と、

上記複数のデータのうち所定のデータに相対する上記固有情報を用いて上記所定のデータを暗号化する暗号化手段と、

暗号化された上記所定のデータ及び上記所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

上記送信手段により送信された上記暗号化された所定のデータ及び上記所定のデータに相対する固有情報を受信する受信手段と、

少なくとも上記受信された上記固有情報を蓄積する第 2 の記憶手段と、

上記暗号化された所定のデータに相対する固有情報により復号化する復号化手段と

を有する端末装置とからなり、

上記固有情報に、更に、時間と共に変化していく時間変化情報を付加し、上記第 2 の記憶手段に記憶されている上記固有情報を所定時間毎に呼び出し、呼び出された上記固有情報が正しいか否かを判断し、上記呼び出された上記固有情報が正しいければ上記固有情報を更新して上記第 2 の記憶手段に戻し、上記呼び出された上記固有情報が正しくなければ上記所定のデータを利用禁止とする

ようにした情報配信システム。

【請求項 6】 上記所定のデータに利用禁止を示す情報を付加して上記所定のデータを利用禁止とするようにした請求項 5 に記載の情報配信システム。

【請求項 7】 上記所定のデータに対する上記固有情報を消去して上記所定のデータを利用禁止とするようにした請求項 5 に記載の情報配信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えば、複数の音楽データが蓄積されるコンテンツサーバと、こ



のコンテンツサーバに蓄積されたコンテンツから所望のコンテンツが配信されるユーザマシンとからなる情報配信システムに関するもので、特に、コンテンツの保護と課金に係わる。

#### 【0002】

##### 【従来の技術】

近年、インターネットや衛星通信の普及により、コンピュータネットワーク網を利用した種々のサービスが実現されつつある。そのようなコンピュータネットワーク網を使ったサービスのひとつとして、以下のような音楽配信サービスを行なうシステムが提案されている。

#### 【0003】

図14において、501はコンテンツサーバ、502はユーザマシンである。コンテンツサーバ501には、複数の音楽データがコンテンツとして蓄積されている。ユーザマシン502には、ハードディスクドライブやMDドライブ等のストレージデバイス504が接続されると共に、課金を行なうためのカードリーダー/ライター505が接続される。カードリーダー/ライター505には、カード506が装着される。

#### 【0004】

音楽配信サービスを利用する場合には、ユーザマシン502が伝送路503を介してコンテンツサーバ501に接続される。伝送路503は、例えば、インターネットのようなコンピュータネットワーク網である。3ユーザマシン502がコンテンツサーバ1に接続されると、コンテンツサーバ501からユーザマシン502にコンテンツのリストや検索画面が送られる。

#### 【0005】

ユーザは、このコンテンツのリストや検索画面で所望のコンテンツを検索して、ダウンロードしたいコンテンツを選択する。ユーザがコンテンツを選択すると、ユーザマシン502からコンテンツサーバ501にそのコンテンツの要求命令が送られる。コンテンツサーバ501で、要求命令に応じてコンテンツが取り出され、このコンテンツがコンテンツサーバ501からユーザマシン502に送られる。そして、このコンテンツがユーザマシン502のストレージデバイス50

4に保存される。このとき、カードリーダー/ライター505により、適切な課金が行なわれる。

#### 【0006】

##### 【発明が解決しようとする課題】

このような音楽配信システムが普及すると、ユーザは、所望の楽曲の音楽データを通信で簡単に入手することができる。また、このようなシステムにおけるサーバには、検索機能が備えられており、このような検索機能を使うと、所望の楽曲を検索して、入手することが簡単にできる。更に、このようなシステムにおけるサーバでは、常に音楽データの更新が行われるため、最新の楽曲をいち早く入手することができる。

#### 【0007】

ところが、このようにサーバからの音楽データをユーザマシンに配信するようなシステムでは、コンテンツのデータが無断で複製され、著作権者の権利が守られなくなる危険性がある。このため、コンテンツのデータが無断で複製されないように、複製防止のための機能を付加する必要があると共に、コンテンツに対して適切な課金が行なわれる必要がある。

#### 【0008】

また、このようなシステムでは、ダウンロードした音楽データを他の機器で再生させたり、他人譲渡したりするようなことが考えられる。常に、1台の機器にのみコンテンツのデータが移動されるようにすれば、不正コピーが出回る可能性はない。ところが、他の機器への複製を一切禁止してしまうと、このようなコンテンツのデータの移動も行なえなくなってしまう。

#### 【0009】

したがって、この発明の目的は、コンテンツの配信を行なうようなシステムで、コンテンツの保護が十分図れ、正当な課金が行なえるようにした情報配信システムを提供することにある。

#### 【0010】

##### 【課題を解決するための手段】

この発明は、複数のデータが蓄積されるとともに複数のデータの各々に相対す

る固有情報が蓄積される第1の記憶手段と、

複数のデータのうち所定のデータに相対する固有情報を用いて所定のデータを暗号化する暗号化手段と、

暗号化された所定のデータ及び所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

送信手段により送信された暗号化された所定のデータ及び所定のデータに相対する固有情報を受信する受信手段と、

少なくとも受信された固有情報を蓄積する第2の記憶手段と、

暗号化された所定のデータに相対する固有情報により復号化する復号化手段と

受信手段により受信された固有情報を第2の記憶手段に予め記憶された他の固有情報と比較する比較手段と、

比較手段の判別に応じて課金処理を行う課金処理手段とを有する端末装置とを備える情報配信システムである。

【0011】

この発明は、複数のデータが蓄積されるとともに複数のデータの各々に相対する固有情報が蓄積される第1の記憶手段と、

複数のデータのうち所定のデータに相対する固有情報を用いて所定のデータを暗号化する暗号化手段と、

暗号化された所定のデータ及び所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

送信手段により送信された暗号化された所定のデータ及び所定のデータに相対する固有情報を受信する受信手段と、

少なくとも受信された固有情報を蓄積する第2の記憶手段と、

暗号化された所定のデータに相対する固有情報により復号化する復号化手段とを有する端末装置とからなり、

固有情報に、更に、時間と共に変化していく時間変化情報を付加し、第2の記

憶手段に記憶されている固有情報を所定時間毎に呼び出し、呼び出された固有情報が正しいか否かを判断し、呼び出された固有情報が正しいければ固有情報を更新して第2の記憶手段に戻し、呼び出された固有情報が正しくなければ所定のデータを利用禁止とする

ようにした情報配信システムである。

#### 【0012】

コンテンツサーバに保存されるコンテンツは、Cキーで暗号化されている。このように、Cキーを設けることにより、コンテンツを移動したり、譲渡したり、再送を要求したりできる。また、送られてきたCキーと同一のCキーがストレージに保存されているか否かを判断することにより、再送か否かを判断して、適切な課金を行なったり、Cキーにランクを付けてコンテンツ毎に料金を変えて課金を行なうようなことができる。

#### 【0013】

また、Cキーに、時間と共に動的に変化するDAコードが付加される。このようなDAコードを付加することで、Cキーを退避させておいて、コンテンツを不正利用するようなことが防止できる。また、この時間と共に動的に変化するDAコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

#### 【0014】

##### 【発明の実施の形態】

以下、この発明の実施の形態について図面を参照して説明する。この発明は、コンテンツのデータを転送するようなシステムにおいて、コンテンツのデータの保護が図れると共に、適切な課金が行なえるようにしたものである。このようなシステムにで用いられる暗号化キーやコードについて先ず簡単に説明しておく。

#### 【0015】

##### 1. キー及びコードの説明

この発明が適用されたシステムでは、以下のような暗号化キーやコードが用いられる。

【0016】

(1) Mキー

M (Machine) キーの役割は、特定の機器でのみデータを利用可能とすることである。Mキーは例えば機器の工場出荷時に各機器毎に与えられるもので、各機器固有の暗号化情報である。Mキーは、保護を図るために、例えば機器の暗号化／復号化処理チップ内に埋め込まれ、機器内から外へは取り出せないようになっている。

【0017】

(2) MIDコード

各機器には、固有のMID (Machine Identification) コードが付与される。このMIDコードも、工場出荷時に各機器に付与される。MIDコードは、各機器を特定するためにのみ使用されるものであり、直接的に暗号化キーとして用いられるものではない。したがって、外部に漏れても、データの保護が守られなくなる危険性は少ない。MIDコードは、Mキーと同様に、例えば機器の暗号化／復号化処理チップ内に埋め込んでおいても良いし、別のROMやEEPROMに蓄えておいても良い。

【0018】

(3) Cキー

C (Contents) キーの役割は、各コンテンツ毎にデータの保護を図ることである。ここで、コンテンツとは、移転できる1かたまりの情報の単位とする。すなわち、データを課金するようなシステムでは、1つの課金の対象となる情報の単位である。音楽サーバのような場合には、1曲毎に課金をするとすると、各曲の音楽データという単位が1つのコンテンツのデータとなる。

【0019】

各コンテンツは、各コンテンツに固有のCキーを用いて暗号化される。したがって、そのコンテンツに対応するCキーを有しているユーザ側の機器でのみ、そのCキーを使ってコンテンツの暗号を解読して、再生することが可能である。このように、Cキーを有しているユーザ側の機器でのみ、そのコンテンツを利用可能なことから、Cキーは、そのコンテンツを利用できる権利を表すキーという見

方もできる。

【0020】

(4) Tキー

T (Transfer) キーの役割は、各ユーザ機器間でデータの移動を行う際に、データの保護を図るためのものである。各機器間でコンテンツの移動を行うような場合に、Cキーが外部に漏れる可能性がある。このため、各機器間でデータの移動を行う場合には、Cキーと、Cキーで暗号化されたコンテンツは、更に、Tキーで暗号化される。

【0021】

Tキーは、データの受け取り側の機器と、データの送り側の機器との間で予め決められたアルゴリズムで、MIDコードに基づいて生成される。すなわち、機器間でコンテンツのデータの転送を行う場合には、受け取り側の機器から送り側の機器に対して、受け取り側のMIDコードが送られる。送り側の機器では、送られてきたMIDコードに基づいて、Tキーが生成される。また、受け取り側の機器では、自分のMIDに基づいて、同様のアルゴリズムによりTキーが生成される。

【0022】

(5) DAコード

暗号/復号化チップ内で生成される動的認証コードであり、Cキーに付加される。DAコードは、例えば、乱数、タイムコード等を利用して生成される。このようなDAコードを付加しておくこと、Cキーを一時的に退避させてコンテンツを不正使用することができなくなる。また、DAコードを利用して、所定の期間使用を許可/禁止したり、コンテンツを貸し借りしたりすることができるようになる。

【0023】

2. Mキーを使ったシステムについて

図1は、この発明が適用されたデータ配信システムの一例を示すものである。この例は、Mキーと呼ばれる暗号化キーを導入して、特定の機器でのみデータを利用可能にするようにしたものである。

## 【0024】

図1において、1はコンテンツサーバ、2はユーザマシン、3はコンテンツサーバ1とユーザマシン2とを結ぶ伝送路である。コンテンツサーバ1には、コンテンツデータベース11が設けられる。このコンテンツデータベース11には、コンテンツサーバ1で提供するコンテンツのデータが格納されている。

## 【0025】

コンテンツデータベース11に格納されるコンテンツのデータは、コンテンツ入力端子13から与えられる。例えば、音楽配信サービスを行なうサーバの場合には、コンテンツ入力端子13から音楽データが与えられる。この音楽データは、エンコーダ14に供給される。エンコーダ14で、この音楽データが例えばATRAC (Adaptive Transform Acoustic Coding) で圧縮符号化される。この圧縮された音楽データがコンテンツデータベース11に蓄えられる。

## 【0026】

また、コンテンツサーバ1には、コード及びキーデータベース12が設けられる。このコード及びキーデータベース12には、コンテンツサーバ1に繋がる全ての機器のユーザマシン2のMIDコードとMキーとが蓄えられる。MIDコードは、各ユーザマシン2を識別するためのユーザマシン毎の固有の情報である。Mキーは、各ユーザマシン毎に固有の暗号化キーである。MIDコード及びMキーは例えば機器の工場出荷時に各ユーザマシン2に与えられる。MIDコード及びMキーを工場出荷時に各ユーザマシン2に付与する際に、各機器毎に付与したMIDコード及びMキーのリストに基づいてコード及びキーデータベース12が作成される。

## 【0027】

コンテンツサーバ1の全体動作は、サーバ処理マネージャ16により管理されている。また、コンテンツサーバ1の通信制御は、通信マネージャ15により管理されている。コンテンツサーバ1からのデータは、暗号化回路17により暗号化される。このときの暗号化は、ユーザマシン2から送られてきたMIDコードに基づいてコード及びキーデータベース12で検索されたMキーにより行なわれる。

## 【0028】

一方、ユーザマシン2には、暗号化／復号化処理チップ21が設けられる。この暗号化／復号化処理チップ21は、データの暗号化処理及び暗号の復号化処理を行う専用のチップである。この暗号化／復号化処理チップ21には、工場出荷時に、機器固有のMIDコードと、Mキーが格納されている。

## 【0029】

図2は、暗号化／復号化処理チップ21の構成を示すものである。暗号化／復号化処理チップ21には、Mキーホルダ51と、MIDコードホルダ52と、Mキー復号化回路53と、コントローラ54が設けられる。Mキーホルダ51には、各機器固有の暗号化情報であるMキーが工場出荷時に記憶される。MIDコードホルダ52には、各機器固有の識別情報であるMIDコードが工場出荷時に記憶される。コントローラ54は、暗号化／復号化処理チップ21の動作を制御している。

## 【0030】

コントローラ54には、コマンド端子CMDからコマンドが与えられる。このコマンドに基づいて、暗号化／復号化処理チップ21の動作が設定される。Mキー復号化回路53には、入力端子DATA\_INからMキーで暗号化されたデータが供給される。また、Mキー復号化回路53には、Mキーホルダ51からMキーが供給される。Mキー復号化回路53で、入力データの暗号解読を行なわれる。Mキー復号回路53の出力は、データ出力端子DATA\_OUTから出力される。また、MIDコードホルダ52からは、コード出力端子MID\_OUTが導出される。このコード出力端子MID\_OUTからは、MIDコードが出力される。

## 【0031】

図2に示すように、暗号化／復号化の処理は、1チップの暗号化／復号化処理チップ21で行われ、この暗号化／復号化処理チップ21内に、Mキーと、MIDコードが格納されている。このため、外部からは、暗号処理がどのようにして行われ、暗号化キーが何であるのかは解明できない。



いる。通信マネージャ15がユーザマシン2からの配信要求、MIDコード、課金情報を受信すると、これら情報は、サーバ処理マネージャ16に送られる。

【0037】

サーバ処理マネージャ16は、ユーザマシン2からMIDコードを受信したら、このMIDコードをコード及びキーデータベース12に送り、そのMIDコードに対応する機器のMキーを問い合わせる。コード及びキーデータベース12は、各機器毎のMIDコードと、これに対応するMキーの情報が予め格納されている。コード及びキーデータベース12は、MIDコードを受け付けると、このMIDコードから機器を識別し、この機器に対応するMキーを出力する。このMキーは、Mキー暗号化回路17に送られる。これにより、Mキー暗号化回路17に、暗号化キーがセットされる。

【0038】

また、サーバ処理マネージャ16は、ユーザマシン2からの配信要求を受け付けると、要求されたコンテンツの配信指示をコンテンツデータベース11に送る。コンテンツデータベース11は、配信指示を受け取ると、要求されたコンテンツのデータの読み出しを行なう。読み出されたコンテンツのデータは、Mキー暗号化回路17に送られる。

【0039】

Mキー暗号化回路17には、コード及びキーデータベース12から、データを要求したユーザマシン2の機器のMIDコードに対応したMキーがセットされている。コンテンツデータベース11から送られるコンテンツのデータは、Mキー暗号化回路17で、このMキーにより暗号化される。そして、このMキーで暗号化されたコンテンツのデータは、コンテンツサーバ1の通信マネージャ15から、通信路3を介して、ユーザマシン2の通信路マネージャ25に送られる。そして、このコンテンツのデータは、ユーザマシン2にあるストレージデバイス20に蓄積される。

【0040】

このように、ユーザマシン2からコンテンツサーバ1にコンテンツのダウンロードを要求する際に、ユーザマシン2からコンテンツサーバ1に、その機器固有

【0032】

図1において、ユーザマシン2には、入力部22から入力を与えられる。入力部22からの入力は、ユーザインターフェース23を介して、マシン処理マネージャ24に与えられる。

【0033】

マシン処理マネージャ24は、ユーザマシン2の全体処理を行っている。マシン処理マネージャ24は、入力部22からコンテンツサーバ1のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理チップ21にコマンドを与え、MIDコードを問い合わせる。暗号化／復号化処理チップ21は、このようなコマンドを受け付けると、このコマンドに対応して、MIDコードホルダ52（図2）に記憶されているMIDコードを出力する。

【0034】

マシン処理マネージャ24は、暗号化／復号化処理チップ21からMIDコードを受け取ったら、通信マネージャ25に、配信要求と、MIDコードと、課金情報を送る。これら配信要求、MIDコード、課金情報は、通信処理マネージャ25から、通信路3を介して、コンテンツサーバ1の通信マネージャ15に送られる。

【0035】

なお、コンテンツサーバ1からのコンテンツの配信サービスを受ける場合には、カード26が装着される。そして、このカード26の残高情報がカードリーダー／ライター27を介してマシン処理マネージャ24に送られる。そして、コンテンツの配信が実行されると、マシン処理マネージャ24は、カードリーダー／ライター27を介して、カード26に、引き出し指示を与え、カード26から、コンテンツの代金が差し引かれる。このようにして、コンテンツに対する代金の支払いが行なわれる。このとき、正規のユーザか否か、ユーザが確かに課金を行っているか否かをチェックしてから、MIDコードに対応するMキーを出力させるようにしても良い。

【0036】

コンテンツサーバ1側では、サーバ処理マネージャ16が全体処理を行なって

のMIDコードが送られる。コンテンツサーバ1には、コード及びキーデータベース12が設けられており、このコード及びキーデータベース12により、ユーザマシン2から送られてきた機器のMIDコードに対応するMキーが呼び出され、コンテンツのデータがこのMキーで暗号化される。そして、機器固有のMキーで暗号化されたコンテンツのデータがユーザマシン2に送られ、ユーザマシン2のストレージデバイス20に蓄えられる。ストレージデバイス20に蓄えられたコンテンツのデータは、機器固有のMキーで暗号化されているので、コンテンツの配信を要求したユーザマシン2以外では復号が行なえない。これにより、コンテンツの著作権を守ることができる。

#### 【0041】

すなわち、ストレージデバイス20に蓄えられたコンテンツのデータを復号する場合には、そのデータは、ストレージデバイス20から、図2における暗号化／復号化処理チップ21のデータ入力端子DATA\_INに送られる。図2に示したように、暗号化／復号化処理チップ21のMキーホルダ51には、その機器固有のMキーが蓄えられている。コンテンツサーバ1から送られてきたコンテンツのデータは、MIDコードホルダ52のMIDコードに対応するMキーで暗号化されているため、コンテンツサーバ1側のMキー暗号化回路17に設定されたMキーは、Mキーホルダ51に格納されているMキーと同様である。したがって、ストレージ20からのMキーで暗号化されたコンテンツのデータは、暗号化／復号化処理チップ21で、復号することができる。

#### 【0042】

これに対して、ストレージデバイス20に蓄えられていたコンテンツのデータを、ユーザマシン2以外の機器に複製したとする。ストレージデバイス20に蓄えられていたコンテンツのデータは、この機器固有のMキーで暗号化されている。他の機器の暗号化／復号化処理チップ21は、この機器と同様のMキーを有していない。このため、ストレージデバイス20に蓄えられていたコンテンツのデータをユーザマシン2以外の機器に複製したとしても、その機器では、コンテンツのデータの暗号を解読できない。

## 【0043】

## 3. Cキーを使ったシステムについて

上述のように、Mキーを導入することで、特定の機器でのみコンテンツのデータが利用可能となる。ところが、Mキーだけでは、その機器からコンテンツのデータを移動させることが一切できなくなってしまう。コンテンツのデータが限りなく複製されてしまうと著作権者の権利が守られなくなることが考えられるが、コンテンツのデータが移動されただけなら、コンテンツのデータを利用する機器が移っただけなので、問題は生じない。Mキーだけでは、このようなコンテンツのデータの移動に対応できない。また、ユーザマシンに一度蓄積しておいたコンテンツのデータがエラーになってしまったり、ダウンロードに失敗したりすることが考えられる。このような場合、正規のユーザが正当な課金をしてそのコンテンツのデータの配信を受けているなら、再度、そのコンテンツのデータを配信し直すことが望まれる。また、コンテンツには有料のコンテンツと無料のコンテンツがあり、Mキーのみでは、コンテンツの種類に応じて適切な課金が行えない。

## 【0044】

このように、Mキーを導入することで、各機器を単位とするデータの保護は図れるが、Mキーだけでは、各コンテンツ毎のデータの保護を図り、適切な課金を行なうには不十分である。そこで、コンテンツ毎の暗号化を行うCキーが導入される。

## 【0045】

図3は、Cキーを導入したシステムの一例を示すものである。Cキーの役割は、各コンテンツ毎にデータの保護を図ることである。

## 【0046】

Cキーを導入したシステムにおいては、ユーザマシン102側の暗号化／復号化処理チップ121として、図4に示すように、Mキーホルダ151と、MIDコードホルダ152と、Mキー復号化回路153と、コントローラ154とが設けられると共に、更に、Cキー取り込み回路155と、Cキー復号化回路156とが設けられる。Mキーホルダ151、MIDコードホルダ152、Mキー復号

化回路153、コントローラ154の動作は、前述のMキーのみのシステムにおける暗号化／復号化処理チップ21と同様であり、Mキーホルダ151には、各機器固有の暗号化情報であるMキーが工場出荷時に記憶され、MIDコードホルダ152には、各機器固有の識別情報であるMIDコードが工場出荷時に記憶され、コントローラ154は、暗号化／復号化処理チップ121の動作を制御している。Cキー取り込み回路155は、Mキーの解読により復号されたCキーを保持するものである。Cキー復号回路156は、Cキーによる復号化処理を行なうものである。

#### 【0047】

コントローラ154には、コマンド端子CMDからコマンドが与えられ、このコマンドに基づいて、暗号化／復号化処理チップ121の動作が設定される。Mキー復号化回路153には、入力端子DATA\_INから、Cキーで暗号化され更にMキーで暗号化されたデータと、入力端子KEY\_INからのMキーで暗号化されたCキーが供給される。また、Mキー復号化回路153には、Mキーホルダ51からMキーが供給される。

#### 【0048】

入力データの暗号化キーがMキーホルダ151からのMキーと一致していれば、Mキー復号化回路153で、暗号解読を行なえる。Mキー復号化回路153からは、Cキーと、Cキーで暗号化されたデータが得られる。このCキーがCキー取り込み回路155に保持される。また、Cキーで暗号化されたデータがCキー復号化回路156に供給される。

#### 【0049】

Cキー復号化回路156で、Cキーの復号が行なわれ、データが解読される。このCキー復号回路156の出力は、データ出力端子DATA\_OUTから出力される。また、MIDコードホルダ152からは、コード出力端子MID\_OUTが導出される。このコード出力端子MID\_OUTからは、MIDコードが出力される。また、Cキーで暗号化されてデータを転送するために、Cキーの出力端子KEY\_OUTと、Cキーで暗号化されたデータの出力端子DATA\_Tが設けられる。

## 【0050】

このように、Cキーを導入したシステムにおいては、図3におけるユーザマシン102側の暗号化／復号化処理チップ121として、図4に示すような構成のものが用いられる。また、図3に示すように、コンテンツサーバ101側には、Cキーを発生するCキー生成部118と、このCキーを使って、コンテンツのデータを暗号化するCキー暗号化回路119が設けられる。それ以外の構成については、前述の図1に示したMキーだけの例と同様である。

## 【0051】

前述のMキーだけのシステム例では、コンテンツ入力端子13からのデータは、エンコーダ14で圧縮符号化されて、そのままコンテンツデータベース11に蓄積されたが、この例では、コンテンツ入力端子113からのデータは、エンコーダ114で圧縮符号化された後、Cキー暗号化回路119に送られ、Cキー生成部118からのCキーにより暗号化されて、コンテンツデータベース111に蓄積される。そして、このときのCキーがコンテンツデータベース111に蓄積される。

## 【0052】

ユーザマシン102のユーザがコンテンツサーバ101のコンテンツの配信を受けたい場合には、入力部122からユーザインターフェース123を介して、マシン処理マネージャ124に入力が与えられる。

## 【0053】

マシン処理マネージャ124は、コンテンツサーバ101のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理チップ121にコマンドを与え、MIDコードを問い合わせる。暗号化／復号化処理チップ121は、暗号化／復号化処理チップ121からコマンドが与えられると、このコマンドに対応して、MIDコードを出力する。

## 【0054】

マシン処理マネージャ124は、MIDコードを受け取ったら、通信マネージャ125に、配信要求と、MIDコードと、課金情報を送る。これらの情報は、通信処理マネージャ125から、通信路103を介して、コンテンツサーバ10

1の通信マネージャ115に送られる。

【0055】

通信マネージャ115は、ユーザマシン102からのMIDコードを受け取ったら、このMIDコードをサーバマネージャ116に送る。サーバマネージャ116は、コード及びキーデータベース112にこのMIDコードを送り、そのMIDコードに対応するMキーを問い合わせる。コード及びキーデータベース112は、このMIDコードに対応する機器のMキーを出力する。コード及びキーデータベース112からのMキーは、Mキー暗号化回路117に送られ、Mキー暗号化回路117にMキーがセットされる。

【0056】

また、サーバ処理マネージャ116は、ユーザマシン102からの配信要求を受け付けると、要求されたコンテンツの配信指示をコンテンツデータベース111に送る。コンテンツデータベース111は、サーバ処理マネージャ116からの情報に基づいて、要求されたコンテンツのデータを読み出す。

【0057】

前述したように、コンテンツデータベース111のデータは、Cキーにより暗号化されている。したがって、Cキーにより暗号化されたコンテンツデータが、更に、Mキー暗号化回路117により、Mキーで暗号化される。また、このときのCキーがコンテンツデータベース111から読み出され、Mキー暗号化回路117により、Mキーにより暗号化される。

【0058】

このように、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーは、コンテンツサーバ101の通信マネージャ115から、通信路103を介して、ユーザマシン102の通信路マネージャ125に送られる。そして、このCキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーは、ストレージデバイス120に蓄積される。

【0059】

このように、コンテンツデータベース111に蓄えられているコンテンツのデ

ータはCキーで暗号化されており、コンテンツサーバ101からユーザマシン102にデータが送られる際に、更に、このデータは、Mキーで暗号化される。したがって、ストレージデバイス120に蓄積されるデータは、Cキーで暗号化され、更に、Mキーで暗号化されている。Cキーで暗号化されたコンテンツのデータを解読するためには、Cキーが必要であるが、このCキーは、コンテンツサーバ1から、Mキーで暗号化されて渡されている。

## 【0060】

ストレージデバイス120に蓄えられたコンテンツのデータを復号する場合に、そのデータは、ストレージデバイス120から、図4における暗号化／復号化処理チップ121のデータ入力端子DATA\_INに送られる。また、Mキーで暗号化されたCキーが、ストレージデバイス120から、暗号化／復号化処理チップ121のキー入力端子KEY\_INに送られる。

## 【0061】

図4に示すように、暗号化／復号化処理チップ121のMキーホルダ151には、その機器固有のMキーが蓄えられている。コンテンツサーバ101から送られてきたコンテンツのデータは、MIDコードホルダ152のMIDコードに対応するMキーで暗号化されているため、コンテンツサーバ101側のMキー暗号化回路117に設定されたMキーは、Mキーホルダ151に格納されているMキーと同様である。したがって、ストレージデバイス120からの、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータは、Mキーについては、Mキー復号化回路153で、復号することができる。

## 【0062】

また、ストレージデバイス120からのMキーで暗号化されたCキーは、Mキー復号化回路153で復号される。

## 【0063】

したがって、Mキー復号化回路153からは、Cキーで暗号化されたデータと、Cキーが出力される。このCキーは、Cキー取り込み回路155に送られ、Cキーで暗号化されたデータは、Cキー復号回路156に送られる。Cキー復号回路156で、Cキーによる解読が行なわれ、データが復号される。この復号され



たデータがデータ出力端子DATA\_\_OUTから出力される。また、Cキーがキー出力端子KEY\_\_OUTから出力される。

【0064】

このようにコンテンツのデータをCキーで暗号化しておく、コンテンツのデータを利用するときには、必ず、これを解読するためのCキーが必要になる。Cキーを有しているユーザ側の機器でのみ、そのコンテンツを利用可能なことから、Cキーは、そのコンテンツを利用できる権利を表すキーとして用いることができる。

【0065】

すなわち、1つの機器から他の機器にCキーを送れば、コンテンツとそのコンテンツを利用する権利が送られたことになり、他のユーザ側の機器で、そのコンテンツが利用可能となる。このように1つの機器から他のユーザ側の機器にCキーを送った後にその機器のCキーを消去してしまうと、たとえ送り側の機器にコンテンツが残っていても、そのコンテンツは最早利用できない。これは、そのコンテンツを譲渡したという見方ができる。

【0066】

また、正規のユーザが誤ってコンテンツを消してしまったり、コンテンツのダウンロードに失敗してしまうような場合がある。この場合でも、Cキーが残っていれば、そのコンテンツを再送してもらい、そのコンテンツを利用することができる。このように、Cキーを導入することにより、以下のように、コンテンツの移動や再送が行なえるようになる。また、Cキーを利用することにより、課金の設定を行なうことができる。

【0067】

暗号化／復号化処理チップ121のキー出力端子KEY\_\_OUTからのCキーと、データの出力端子DATA\_\_TからのCキーで暗号化されたデータを相手側の機器に転送し、転送が終わったら、Cキー取り込み回路155に保存されているCキー及びストレージデバイス120に保存されているCキーを消去することで、コンテンツの移動が行なわれる。このようにすると、相手側の機器でのみコンテンツの利用が可能となる。このとき、ストレージデバイス120に残ってい

一致するか否かが判断される（ステップS4）。受信されたCキーと、ストレージデバイス120に保存されているCキーとが一致している場合には、再送であるので、課金は行なわれない（ステップS2）。

## 【0071】

ステップS3でストレージデバイス120にCキーが保存されていないと判断された場合、又はステップS4で、受信されたCキーとストレージデバイス120に保存されているCキーとが一致していないと判断された場合には、Cキーの課金ランクが取得される（ステップS5）。そして、この課金ランクに応じて、課金処理が行なわれる（ステップS6）。

## 【0072】

## 4. Tキーを使ったシステムについて

このように、Cキーを導入することで、コンテンツのデータの移動、再送が行なえるようになる。ところが、Cキーのみでは、相手側の機器にコンテンツの移動を行なう際に、Cキーが直接転送される。このとき、Cキーが外部に漏れて、コンテンツのデータの保護が図られなくなる可能性がある。そこで、データを転送時のコンテンツのデータの保護を図るために、Tキーが導入される。

## 【0073】

図6は、Tキーを導入したシステムの一例を示すものである。図6において、データの送り側のユーザマシン202Aは、ストレージデバイス220A、暗号化／復号化処理チップ221A、入力部222A、ユーザインターフェース223A、マシン処理マネージャ224A、通信マネージャ225A、カードリーダー／ライター227Aから構成される。カードリーダー／ライター227Aには、カード226Aが装着される。

## 【0074】

データの受信側のユーザマシン202Bは、ストレージデバイス220B、暗号化／復号化処理チップ221B、入力部222B、ユーザインターフェース223B、マシン処理マネージャ224B、通信マネージャ225B、カードリーダー／ライター227Bから構成される。カードリーダー／ライター227Bには、カード226Bが装着される。

るコンテンツのデータは、消去しなくても良い。なぜなら、ストレージデバイス120に残っているコンテンツのデータは、Cキーで暗号化されており、Cキーが消去されてしまえば、そのコンテンツのデータは利用できないからである。

## 【0068】

ストレージデバイス120のコンテンツのデータを消去してしまった後でも、Cキーが保存されていれば、コンテンツの再送が行なえる。コンテンツの再送は、前述のコンテンツデータのダウンロードの場合と同様の処理で行なわれる。このとき、新規のダウンロードであるか否かをCキーで判断し、新規の場合のみ、課金を行なうようにする。

## 【0069】

Cキーを使うと、コンテンツに応じた課金が行なえる。例えば、無料のコンテンツに対してはCキーを付加せず、有料のコンテンツにのみCキーを付加する。そして、受信側では、送られてきたCキーが新規のものであるか否かを判断し、新規のCキーの場合のみ、課金を行なうようにする。このようにすると、Cキーから、有料のコンテンツか否かを判断することができ、有料のコンテンツの保護が図れる。また、上述のコンテンツの再送のような場合には、保存されているCキーと、受信されたコンテンツを暗号化するためのCキーとを比較し、この比較結果から、課金を行なうかどうかを判断することができる。更に、課金に関する情報（例えば、コンテンツのランク付け等）をコード化してCキーに包含させておき、同じコンテンツに対して条件により料金を変更できるようにすることも可能である。

## 【0070】

図5は、Cキーを使った課金処理を示すフローチャートである。ダウンロードの際に、Cキーが受信されたか否かが判断される（ステップS1）。Cキーが受信されなければ、無料のコンテンツであるとして、課金は行なわれない（ステップS2）。Cキーが受信されたら、ストレージデバイス120にCキーが保存されているか否かが判断される（ステップS3）。コンテンツの再送のような場合には、ストレージデバイス120にCキーが残されている。このような場合には、受信されたCキーと、ストレージデバイス120に保存されているCキーとが

する際には、データを送出する側のユーザマシン202Aから相手側のユーザマシン202BにMIDコードの転送要求が送られる。

【0080】

相手側のユーザマシン202Bでは、MIDコードの転送要求を受け付けると、ユーザマシン202Bの暗号化／復号化処理チップ221BのMIDホルダ252からMIDコードを呼び出し、このMIDコードをコード出力端子MID\_\_OUTから出力させる。そして、このMIDコードは、ユーザマシン202Bから、ユーザマシン202Aに送られる。

【0081】

データを送出する側のユーザマシン202Aでは、コード入力端子MID\_\_INから相手側のユーザマシン202BからのMIDコードを受け付けると、このMIDコードをTキー生成回路258Aにセットする。Tキー生成回路258Aは、この相手側のユーザマシン202Bから送られてきたMIDコードに基づいて、Tキーを生成する。このTキーがTキー暗号化回路257Aにセットされる。

【0082】

ユーザマシン202BからのMIDコードを受け付け、Tキー暗号化回路257AにこのMIDコードに基づくTキーがセットされたら、ユーザマシン201Aからユーザマシン201Bへのコンテンツのデータ及びCキーの転送が開始される。

【0083】

ユーザマシン202Aのストレージデバイス220Aには、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーが蓄積されている。したがって、ユーザマシン202Aからユーザマシン202Bにコンテンツのデータ及びCキーを転送する際に、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーが、ユーザマシン202Aのストレージデバイス220Aから、暗号化／復号化処理チップ221Aのキー入力端子KEY\_\_IN及びデータ入力端子DATA\_\_INに入力される。

## 【0084】

Mキー復号化回路253Aには、Mキーホルダ251AからMキーが供給される。Mキー復号化回路253Aで、Mキーホルダ251AからのMキーによりMキーの復号が行なわれる。このMキー復号回路253Aからは、Cキーと、Cキーで暗号化されたコンテンツのデータが出力される。Cキーは、Cキー取り込み回路255Aに供給されると共に、Tキー暗号化回路257Aに供給される。Cキーで暗号化されたコンテンツのデータは、Cキー復号化回路256Aに供給されると共に、Tキー暗号化回路257Aに供給される。

## 【0085】

Cキー復号化回路256Aで、Cキーの復号化処理が行なわれ、コンテンツのデータが復号される。復号されたデータは、データ出力端子DATA\_\_OUTから出力される。

## 【0086】

Tキー暗号化回路257Aには、Tキー生成回路258AからTキーが供給される。Tキー生成回路258Aには、ユーザマシン202BのMIDコードに基づいて生成されたTキーが設定されている。Mキー復号回路253AからのCキー及びCキーで暗号化されたコンテンツのデータは、Tキー暗号化回路257Aで、相手側のユーザマシン202BのMIDコードに基づいて生成されたTキーで暗号化される。したがって、Tキー暗号化回路257Aからは、Tキーで暗号化されたCキーと、Cキーで暗号化され更にTキーで暗号化されたコンテンツのデータが出力される。

## 【0087】

このTキーで暗号化されたCキーと、Cキーで暗号化され更にTキーで暗号化されたコンテンツのデータは、キー出力端子TKEY\_\_OUT及びデータ出力端子TDATA\_\_OUTから出力され、相手側のユーザマシン202Bに送られ、相手側のユーザマシン202Bの暗号化／復号化処理チップ221Bのキー入力端子RCKEY\_\_IN及びデータ入力端子RDATA\_\_INに入力され、そして、Tキー復号化回路260Bに供給される。

## 【0088】

Tキー復号化回路260Bには、Tキー生成回路259Bから、Tキーが与えられる。このTキーは、MIDホルダ252BからのMIDコードに基づいて生成されている。

## 【0089】

送り側のユーザマシン202Aでは、ユーザマシン202BからのMIDコードを受信し、Tキー生成回路258Aで、このMIDコードに基づいて、Tキーを生成している。受信側のTキー復号化回路260Bでは、MIDコードホルダ252BからのMIDコードに基づいてTキーを生成している。Tキー生成回路258Aと259Bには、共に、同一のMIDコードが送られている。したがって、ユーザマシン202Aから送られてきたコンテンツのデータ及びCキーは、ユーザマシン202BのTキー復号回路260Bで復号することができる。

## 【0090】

Tキー復号化回路260Bからは、Cキーと、Cキーで暗号化されたコンテンツのデータが出力される。このCキーと、Cキーで暗号化されたコンテンツのデータは、Mキー暗号化回路261Bに供給される。

## 【0091】

Mキー暗号化回路261Bには、Mキーホルダ251Bから、機器固有のMキーが与えられる。このMキーにより、Cキーと、Cキーで暗号化されたコンテンツのデータは、暗号化される。したがって、Mキー暗号化回路261Bからは、Mキーで暗号化されたCキーと、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータが出力される。このMキーで暗号化されたCキーと、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータは、キー出力端子RKEY\_OUT及びデータ出力端子RDATA\_OUTから出力され、ユーザマシン202Bのストレージデバイス220Bに保存される。

## 【0092】

このように、Tキーを用いると、ユーザマシン202Aからユーザマシン202Bにデータを転送する際に、ユーザマシン202Aからユーザマシン202Bに送られるCキー及びCキーで暗号化されたコンテンツのデータは、更にTキー

で暗号化される。このため、外部に暗号化キーが漏れることがなく、コンテンツのデータの保護が図れる。

【0093】

#### 5. DAコードを用いてシステム

このように、Tキーを導入すると、異なる機器間にデータを移動させる際のデータ保護を図ることができる。しかしながら、Tキーを導入したとしても、同一の機器内でデータを移動することは可能である。このため、Cキーを同一機器内の別の場所に一時的に保存しておいてから、コンテンツのデータの移動を行ない、その後に、Cキーを元に戻すようなことを行なうと、コンテンツのデータが不正に複製されてしまう。

【0094】

そこで、Cキーに、時間と共に動的に変化するコード（DAコードと称する）を付加して、Cキーに時間的に変化する要素を持たせることが考えられる。

【0095】

つまり、図9において、ユーザマシン302は、ストレージデバイス320、暗号化／復号化処理チップ321、入力部322、ユーザインターフェース323、マシン処理マネージャ324、通信マネージャ325、カードリーダー／ライタ327から構成される。カードリーダー／ライタ327には、カード326が装着される。

【0096】

このような機器で、例えばストレージデバイス320からCキーを読み出し、このCキーをCキー保存メモリ330に保存しておいてから、ストレージデバイス320のコンテンツのデータを他の機器に移動したとする。この場合、データの移動が終了すると、ストレージデバイス320のCキーは消されるが、Cキー保存メモリ330にCキーを退避させておけば、このCキーは消去されない。その後、Cキー保存メモリ330からのCキーをストレージデバイス320に戻せば、ストレージデバイス320にコンテンツのデータがあれば、このコンテンツのデータを復号できてしまう。また、ストレージデバイス320にコンテンツデータが無くても、Cキーがあれば、コンテンツデータの再送が要求できる。

## 【0097】

そこで、図10に示すように、Cキーに対して、時間と共に動的に変化するDAコードが付加される。このDAコードとしては、タイムコードや乱数が用いられる。このように、Cキーに対してDAコードを付加することにより、コンテンツの不正利用を防止することができる。

## 【0098】

図11は、DAコードが付加されたCキーを扱うための暗号化／復号化処理チップ321の構成を示すものである。図11に示すように、暗号化／復号化処理チップ321には、Mキーホルダ351と、MIDホルダ352と、Mキー復号化回路353と、コントローラ354と、Cキー取り込み回路355と、Cキー復号化回路356と、Tキー暗号化回路357と、Tキー生成回路358、359と、Tキー復号化回路360と、Mキー暗号化回路361とが設けられると共に、DAコード管理回路362とが設けられる。

## 【0099】

DAコード管理回路362は、Cキーに付加するDAコードの管理を行なうものである。すなわち、DAコード管理回路362は、所定時間毎にストレージデバイス320からのCキーを呼び出しを行なう。Cキーが呼び出されると、DAコードのチェックを行い、DAコードが正しければ、DAコードの更新処理を行なう。

## 【0100】

なお、ストレージデバイス320には、Mキーで暗号化されたCキーが保存されている。したがって、このMキーで暗号化されたCキーは、先ず、キー入力端子KEY\_INから、Mキー復号化回路353に送られて、復号される。Mキー復号化回路353から、Cキーが出力され、このCキーは、DAコード管理回路362に送られる。

## 【0101】

DAコード管理回路362は、このDAコードを所定時間毎に検出して正しく更新されているDAコードが付加されているか否かを判断し、正しく更新されているDAコードなら、DAコードの更新を行なう。そして、このDAコードを更



新したCキーをMキー暗号化回路361に送って暗号化して、再び、ストレージデバイス320に保存する。

#### 【0102】

図12は、DAコード管理回路362の処理を示すフローチャートである。図12において、所定時間経過したか否かが判断され（ステップS11）、所定時間経過したら、Cキーが呼び出され、Cキーに付加されているDAコードが検出される（ステップS12）。そして、このDAコードが正しく更新されているDAコードであるか否かが判断される（ステップS13）。DAコードが正しく更新されているか否かは、チップ31内に保持しているDAコードとストレージデバイス320から読み出されたDAコードが一致しているか否かにより判断できる。ステップS13で正しく更新されているDAコードであると判断されると、このDAコードが次のDAコードに更新され、そして、この更新されたDAコードが付加されたCキーは、再び、ストレージデバイス320に戻される（ステップS14）。

#### 【0103】

ステップS13で、検出されたDAコードが正しく更新されているDAコードではないと判断されたら、Cキーを消去し、又は、Cキーに不正利用を示すコードを付加して、そのコンテンツの利用が禁止される（ステップS15）。

#### 【0104】

このように、ストレージデバイスのCキーが正常に扱われている場合には、DAコード管理回路362で、Cキーに付加されるDAコードが絶えず更新され、更新されたDAコードが付加されたCキーがストレージデバイス320に保存される。

#### 【0105】

例えば、Cキーを図9におけるCキー保存メモリ330に保存しておいたような場合には、CキーのDAコードが更新されないで、DAコード管理回路362で、DAコードが正しくないと判断される。これにより、コンテンツのデータの不正利用が防止できる。

## 【0106】

なお、このような動的に変化するDAコードを使うと、ある期間再生を禁止／許可することができるようになる。これを利用すると、コンテンツを所定の期間貸し出したり、コンテンツの利用に試用期間を設定したりすることができる。

## 【0107】

図13は、所定期間だけ再生可能に設定する場合の処理を示すフローチャートである。なお、この場合、DAコードとして、タイムコードが用いられる。また、このCキーに、更に、期限情報が付加される。

## 【0108】

図13において、所定時間経過したか否かが判断され（ステップS21）、所定時間経過したら、ストレージデバイスに保存されているCキーが呼び出される。そして、このCキーに付加されているDAコードが検出される（ステップS22）。そして、DAコードが正しく更新されているか否かが判断される（ステップS23）。ステップS23で正しく更新されているDAコードであると判断されると、このDAコードが次のDAコードに更新される（ステップS24）。そして、この更新されたDAコードと期限情報とが比較され、期限超過か否かが判断される（ステップS25）。期限超過でなければ、この更新されたDAコードが付加されたCキーがストレージデバイスに戻され（ステップS26）、ステップS21リターンされる。

## 【0109】

ステップS23で、ストレージデバイスから呼び出されたDAコードが正しく更新されているものではないと判断されたら、このCキーが削除され、又は、不正使用を示すコードが付加されて、利用不可能とされる。（ステップS26）。また、ステップS25で、期間超過であると判断されると、ステップS26に行き、Cキーが削除され、又は、不正使用を示すコードが付加されて、利用不可能とされる。

## 【0110】

このようにして、DAコードを用いて、ある期間再生を禁止／許可したりすることができる。これにより、試用期間を設けて、データを再生させるようなこと

ができる。更に、一方のユーザマシンから他方のユーザマシンにコンテンツのデータを移動する場合に、一方のユーザマシンのCキーをDAコードにより所定の期限まで再生禁止とし、他方のユーザマシンのCキーをその期間のみ再生可能とすると、一方のマシンから他方のマシンに所定の期間だけコンテンツのデータを貸すような制御が行なえる。

#### 【0111】

##### 【発明の効果】

この発明によれば、コンテンツサーバに保存されるコンテンツは、Cキーで暗号化されている。このように、Cキーを設けることにより、コンテンツを移動したり、再送を要求したりできる。また、送られてきたCキーと同一のCキーがストレージデバイスに保存しているか否かを判断することにより、再送か否かを判断して、適切な課金を行なったり、Cキーにランクを付けてコンテンツ毎に料金を変えて課金を行なうようなことができる。

#### 【0112】

また、この発明によれば、Cキーに、時間と共に動的に変化するDAコードが付加される。このようなDAコードを付加することで、Cキーを退避させておいて、コンテンツを不正利用するようなことが防止できる。また、この時間と共に動的に変化するDAコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

##### 【図面の簡単な説明】

#### 【図1】

この発明が適用できるデータ配信システムにおけるMキーを用いたシステムの説明に用いるブロック図である。

#### 【図2】

この発明が適用できるデータ配信システムにおけるMキーを用いたシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

#### 【図3】

この発明が適用できるデータ配信システムにおけるCキーを用いたシステムの説明に用いるブロック図である。

【図 4】

この発明が適用できるデータ配信システムにおける C キーを用いたシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

【図 5】

この発明が適用できるデータ配信システムにおける C キーを用いたシステムの説明に用いるフローチャートである。

【図 6】

この発明が適用できるデータ配信システムにおける T キーを用いたシステムの説明に用いるブロック図である。

【図 7】

この発明が適用できるデータ配信システムにおける T キーを用いたシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

【図 8】

この発明が適用できるデータ配信システムにおける T キーを用いたシステムにおける暗号化／復号化処理チップの説明に用いるブロック図である。

【図 9】

この発明が適用できるデータ配信システムにおける D A コードを用いたシステムの説明に用いるブロック図である。

【図 10】

D A コードの説明に用いる略線図である。

【図 11】

この発明が適用できるデータ配信システムにおける D A コードを用いてシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

【図 12】

この発明が適用できるデータ配信システムにおける D A コードを用いたシステムの説明に用いるフローチャートである。

【図 13】

この発明が適用できるデータ配信システムにおける D A コードを用いたシステムの説明に用いるフローチャートである。

## 【0075】

Tキーを導入したシステムでは、暗号化／復号化処理チップ221A及び221Bとして、図7に示すようなものが用いられる。図7に示すように、暗号化／復号化処理チップ221A及び221Bには、Mキーホルダ251と、MIDコードホルダ252と、Mキー復号化回路253と、コントローラ254と、Cキー取り込み回路255と、Cキー復号化回路256とが設けられると共に、Tキー暗号化回路257と、Tキー生成回路258、259と、Tキー復号化回路260と、Mキー暗号化回路261とが設けられる。

## 【0076】

Mキーホルダ251、MIDコードホルダ252、Mキー復号化回路253、コントローラ254の動作は、前述までのシステムにおける暗号化／復号化処理チップ21、121と同様であり、Mキーホルダ251には、各機器固有の暗号化情報であるMキーが工場出荷時に記憶され、MIDコードホルダ252には、各機器固有の識別情報であるMIDコードが工場出荷時に記憶され、コントローラ254は、暗号化／復号化処理チップ221A、221Bの動作を制御している。また、Cキー取り込み回路255は、Mキーの解読により復号されたCキーを保持し、Cキー復号回路256は、Cキーの復号化処理を行なう。

## 【0077】

Tキー暗号化回路257は、Tキー生成回路258からのTキーにより、転送するデータをTキーで暗号化するものである。Tキー復号回路260は、Tキー生成回路259からのTキーにより、転送されてきたデータを復号するものである。なお、Tキー生成回路258及び259は、MIDコードに基づいてTキーを生成するものであり、そのアルゴリズムは同一である。

## 【0078】

図6において、ユーザマシン202Aからユーザマシン202Bに、コンテンツのデータを移動するとする。図8は、このときの暗号化／復号化処理チップ221A、221Bの動作を説明するためのものである。

## 【0079】

ユーザマシン202Aからユーザマシン202Bにコンテンツのデータを移動

【図 14】

従来のデータ配信システムの一例のブロック図である。

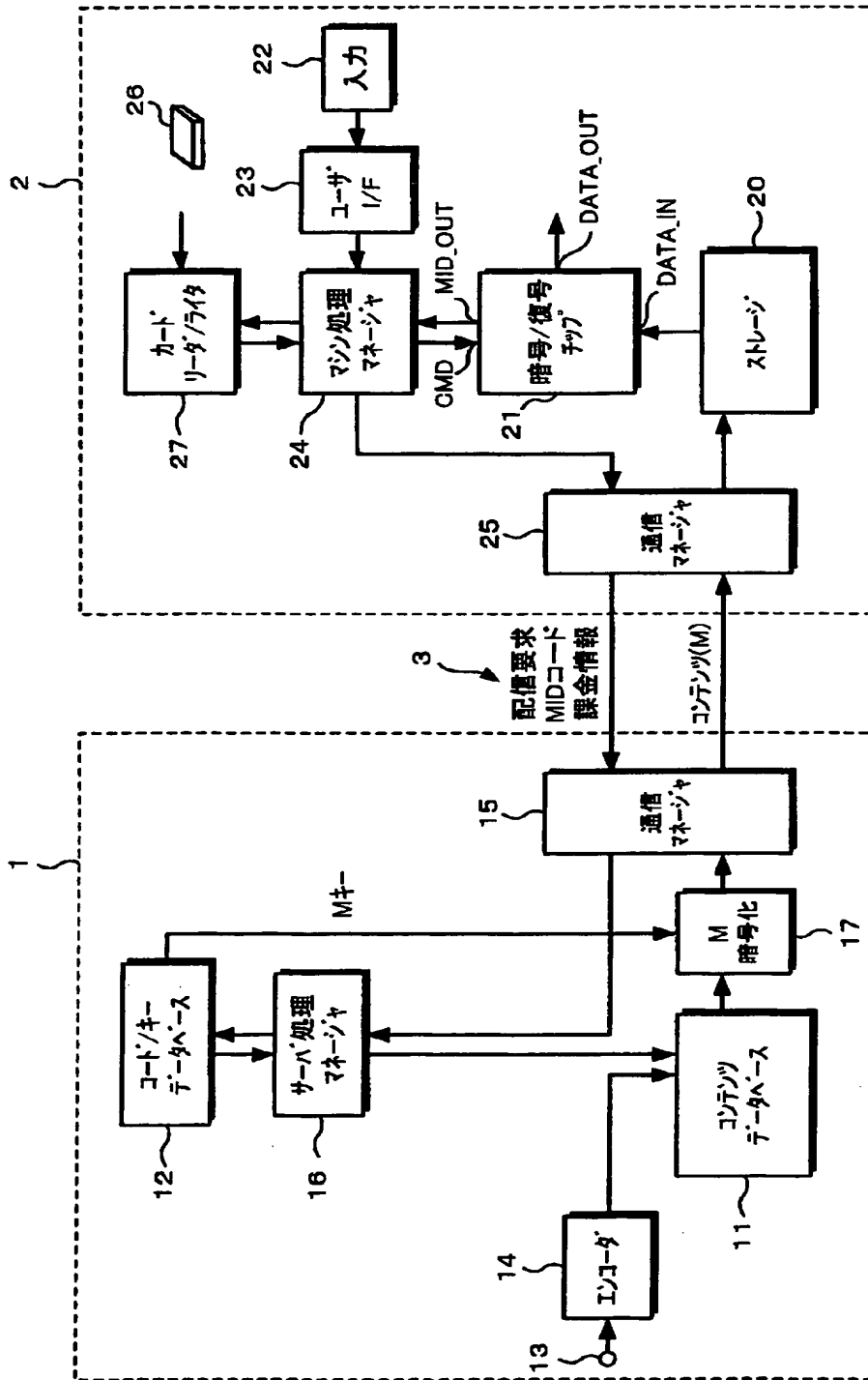
【符号の説明】

1、101・・・コンテンツサーバ、2、102、202A、202B、302  
・・・ユーザマシン、20、120、220A、220B、320・・・ストレ  
ージデバイス、21、121、221A、221B、321・・・暗号化／復号  
化処理チップ

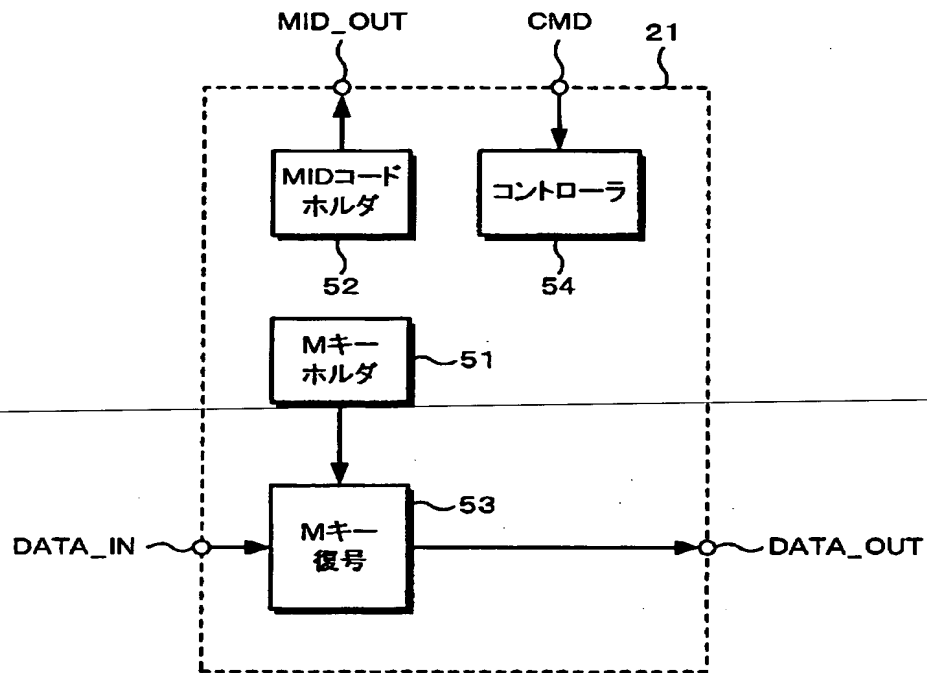
---

【書類名】 図面

【図 1】

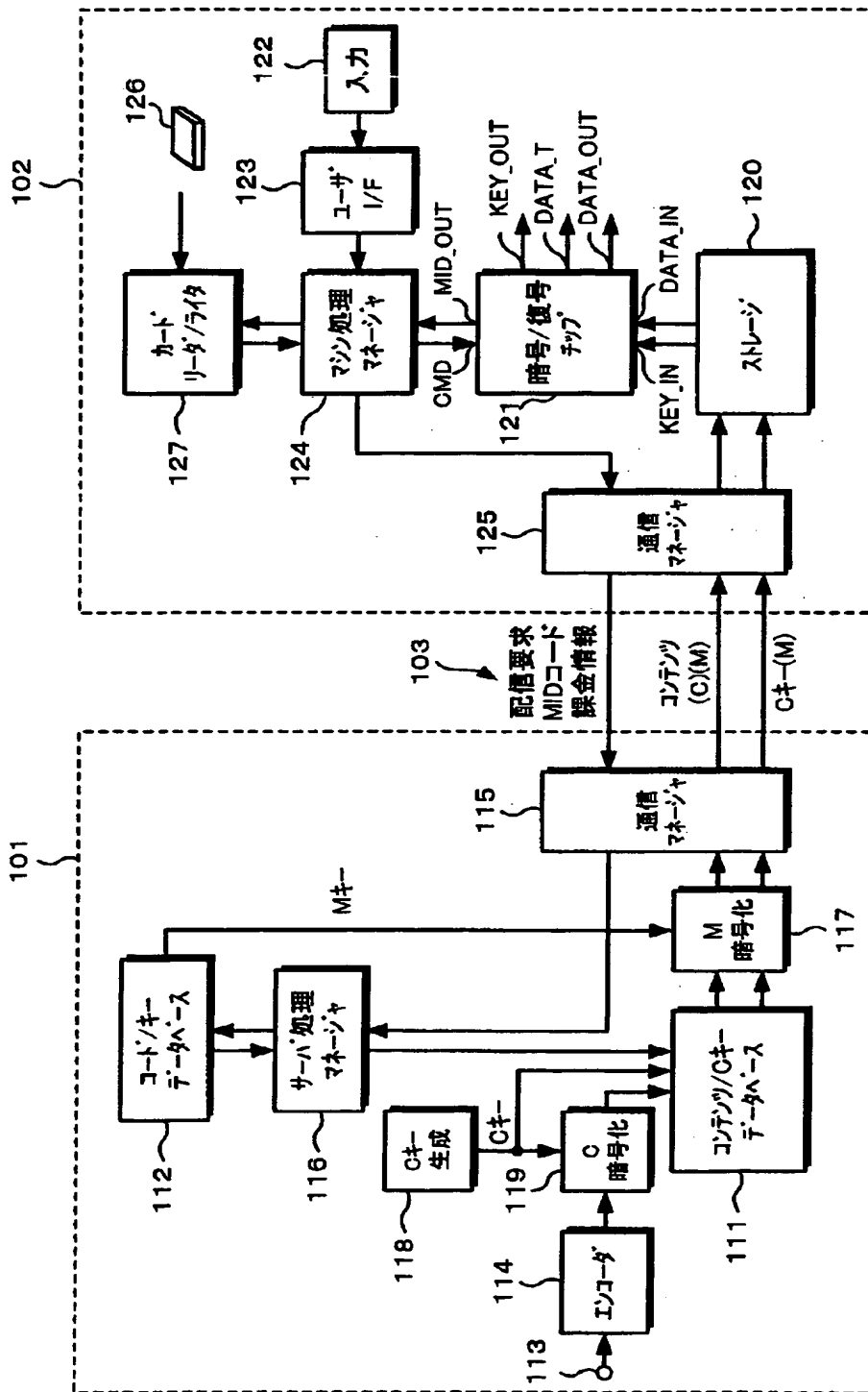


【図 2】

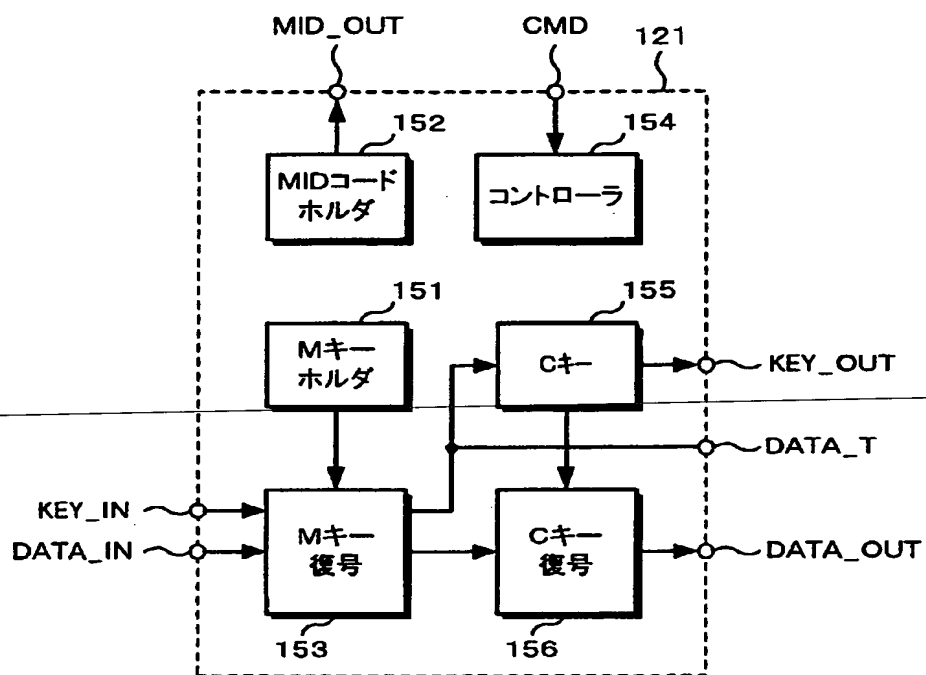




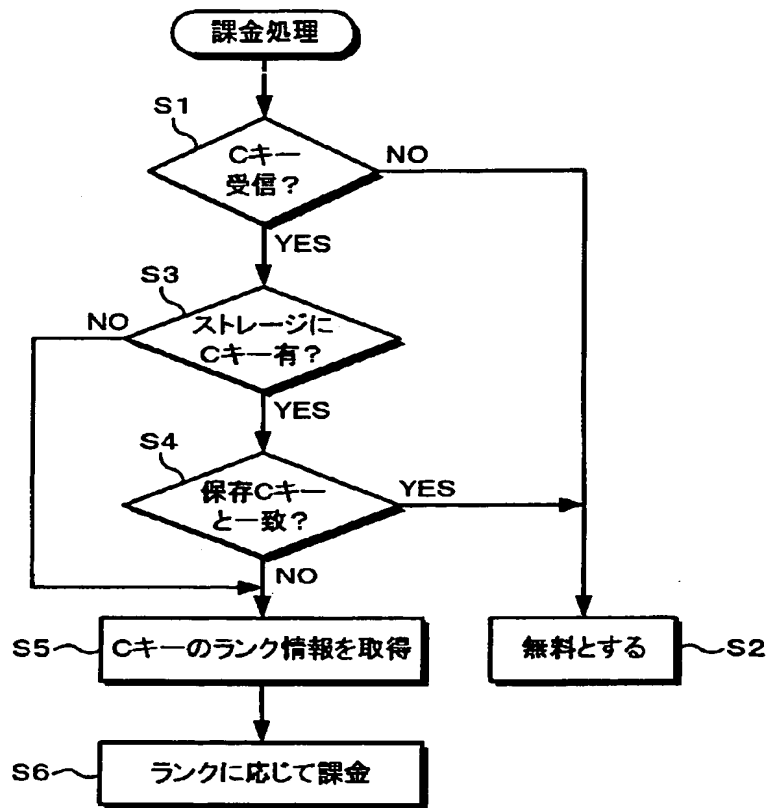
【図 3】



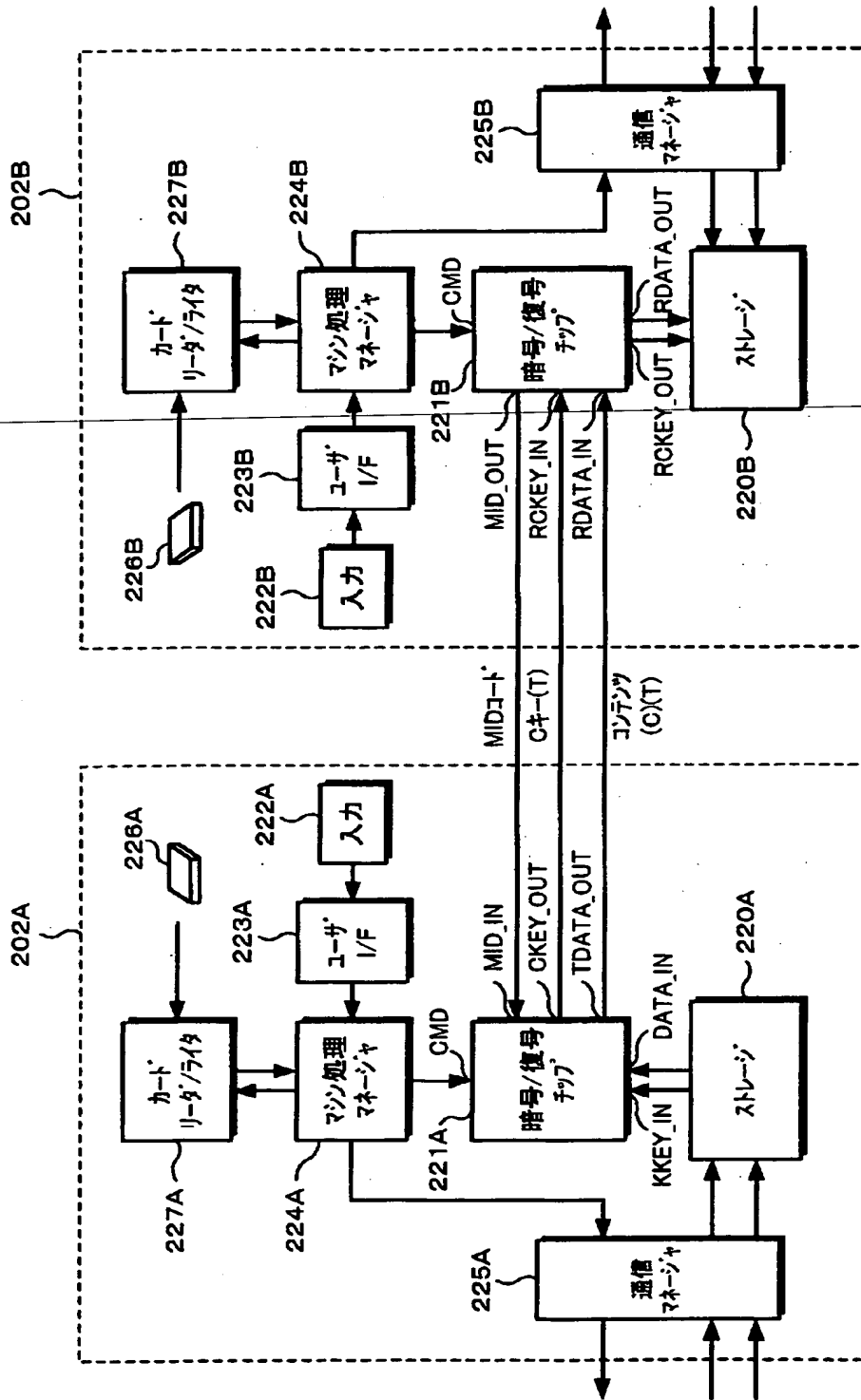
【図4】



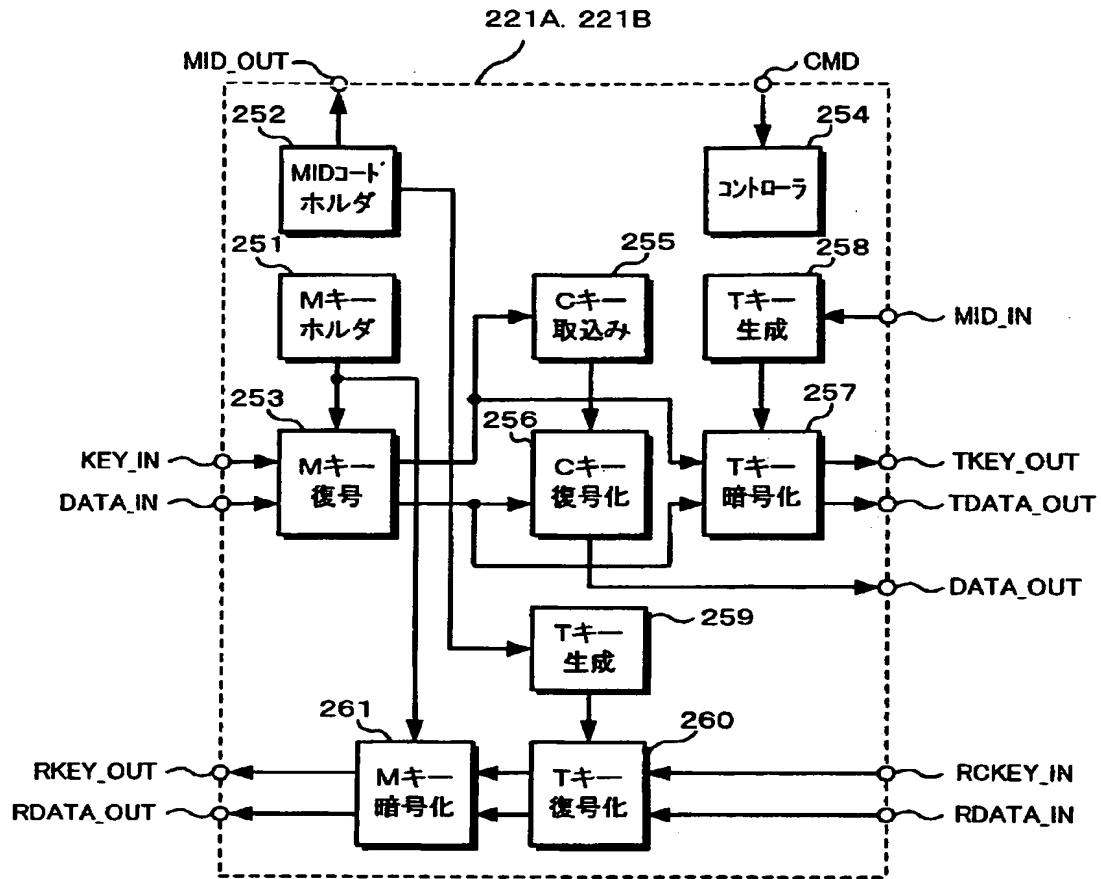
【図5】



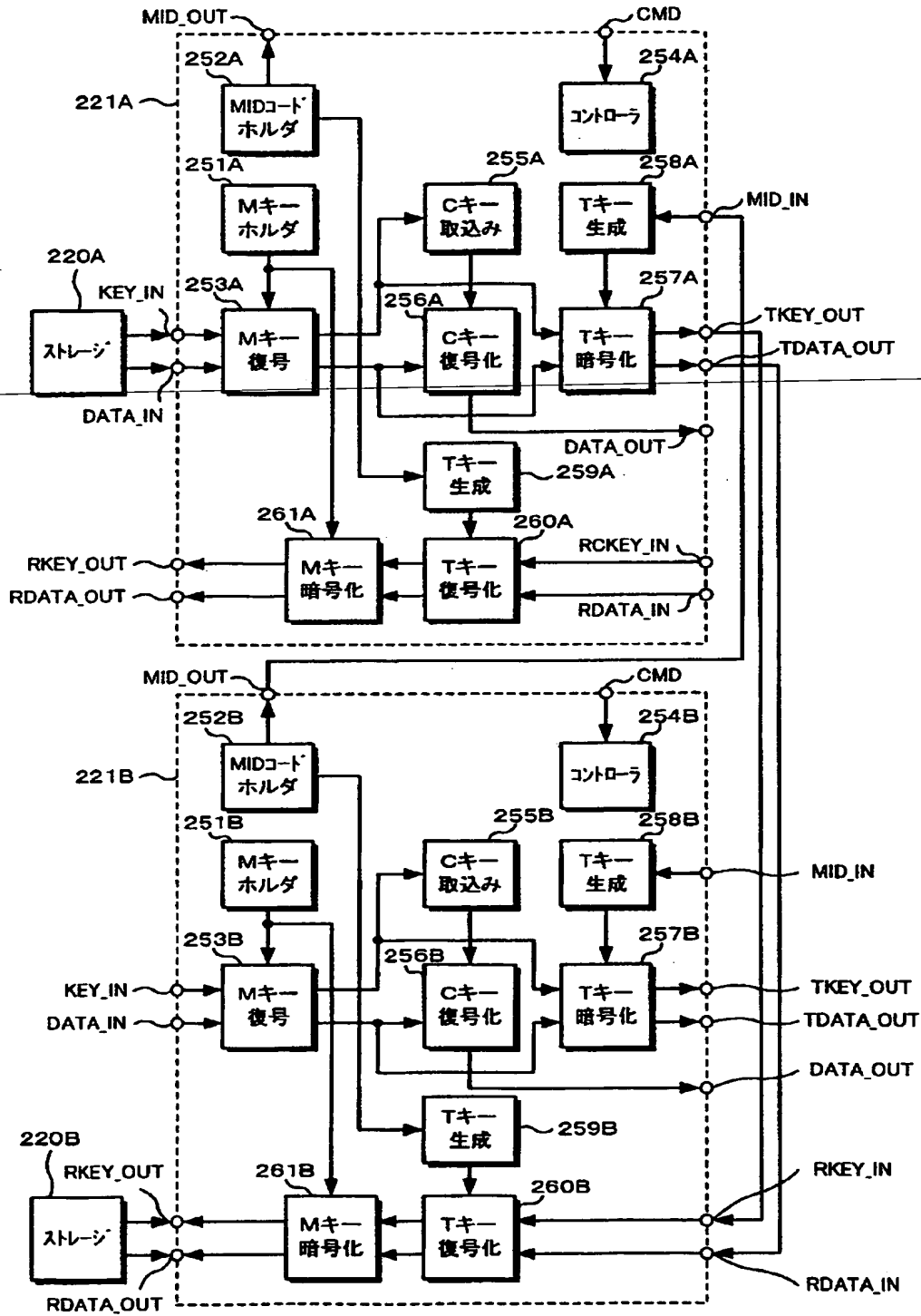
【図6】



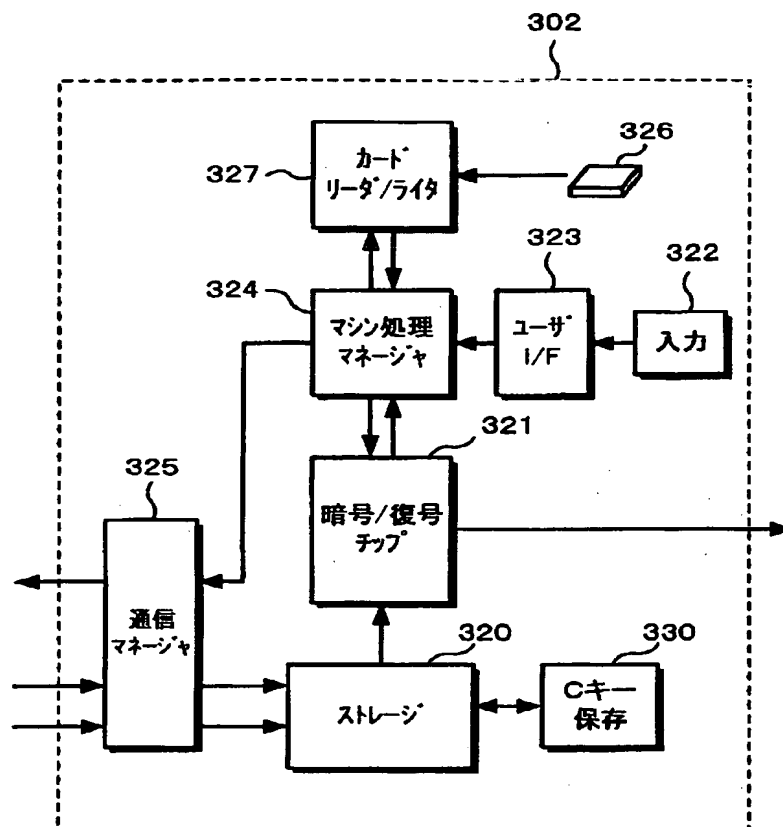
【図 7】



【図 8】



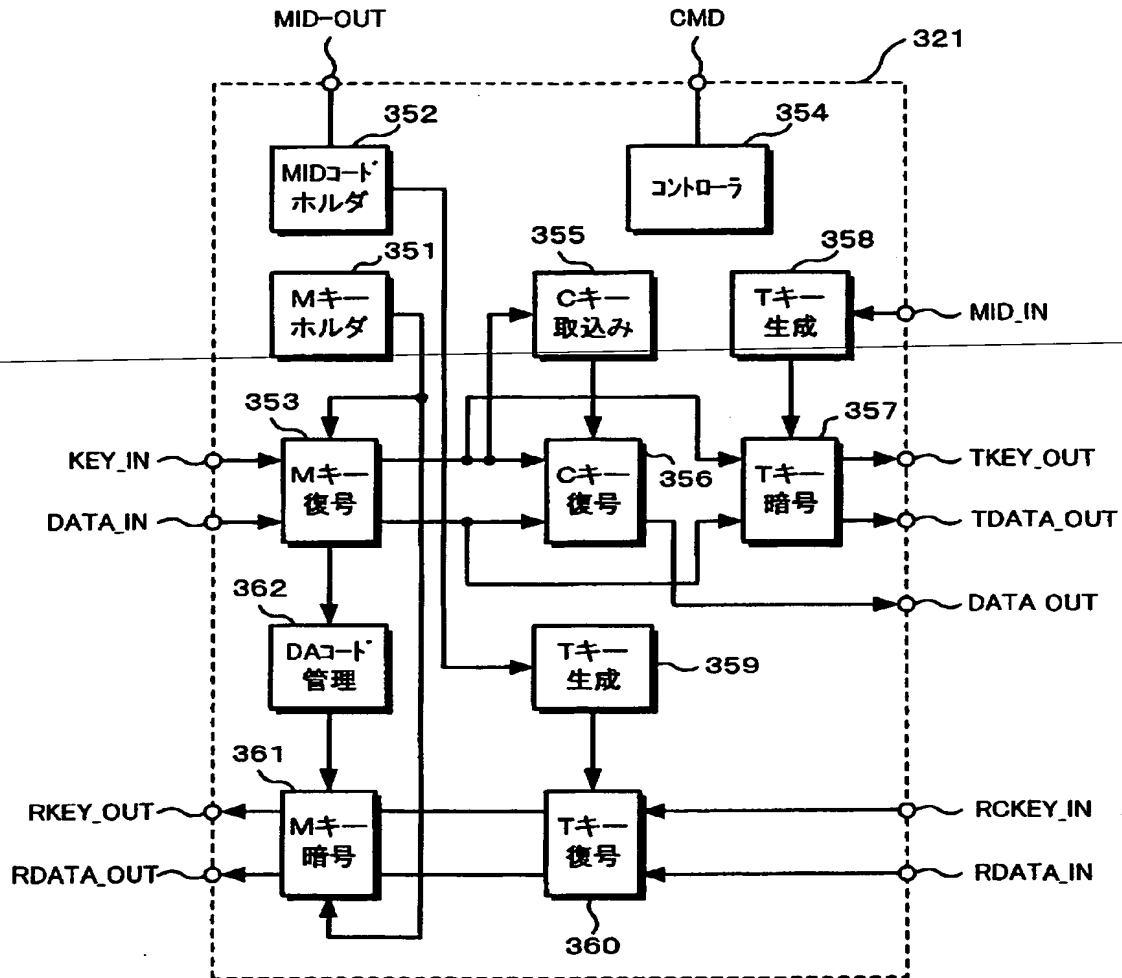
【図 9】



【図 10】

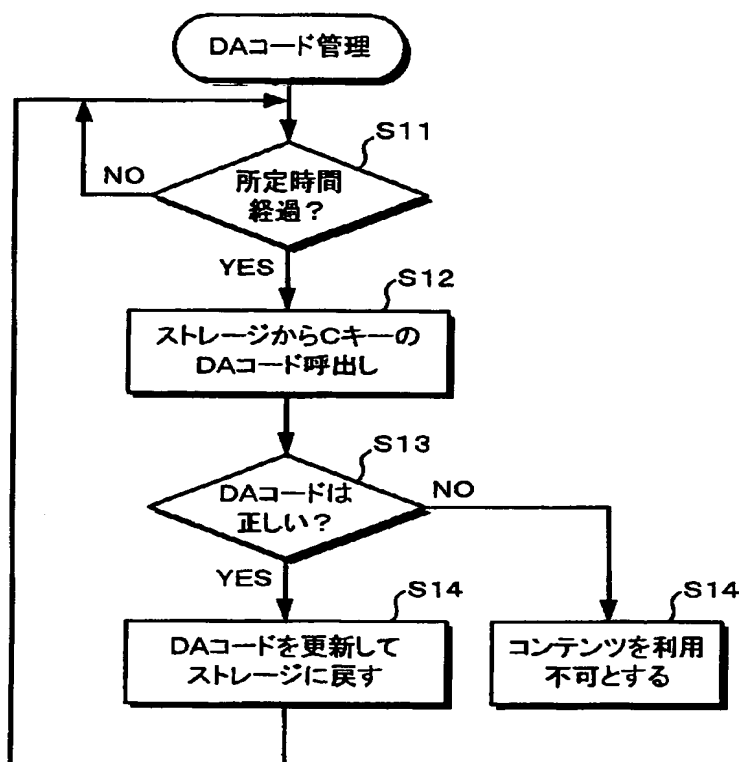


【図 11】

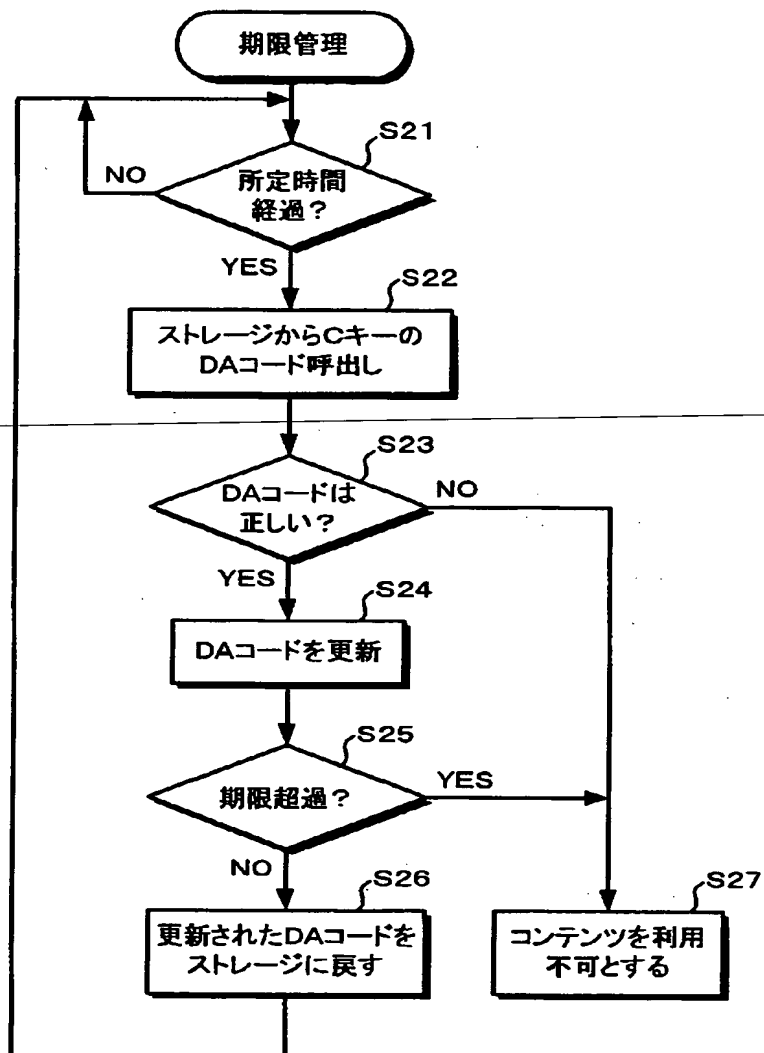




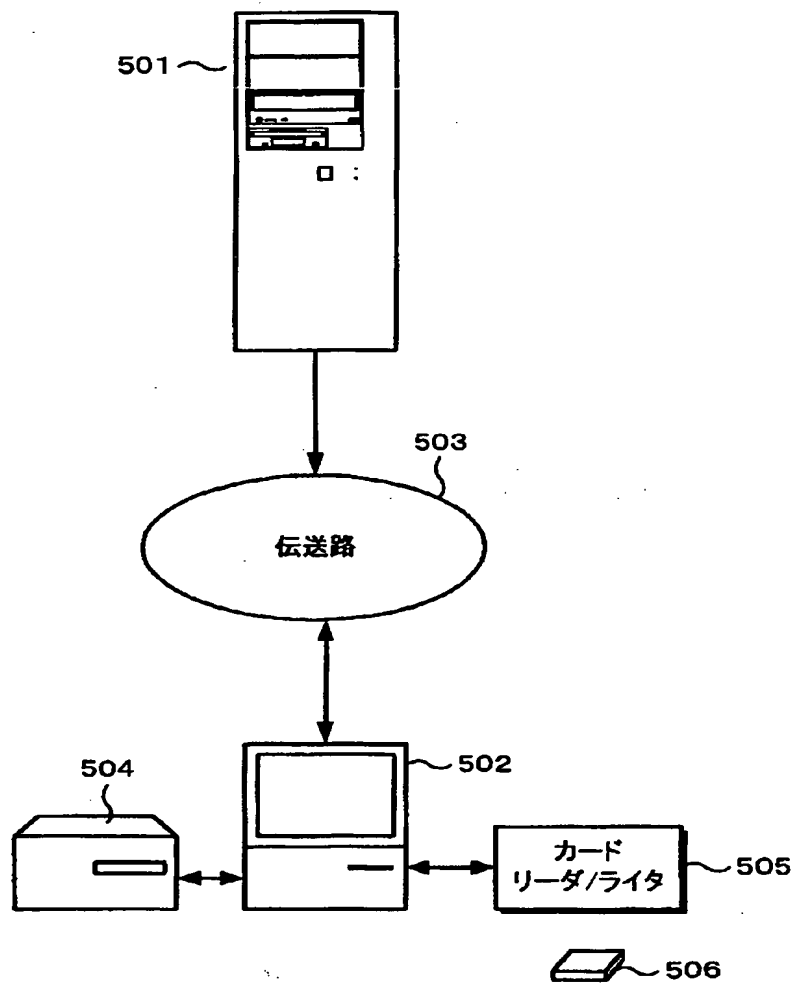
【図 12】



【図13】



【図 14】



---

**THIS PAGE BLANK (USPTO)**